Active Authentication

Beyond Passwords

Richard Guidorizzi, I2O Program Manager

18 Nov 2011

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **18 NOV 2011**	2. REPORT TYPE	3. DATES COVERED **00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE **Active Authentication Beyond Passwords**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Advanced Research Projects Agency (DARPA),675 North Randolph Street,Arlington,VA,22203-2114**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented during DARPA Active Authentication Proposer Day - November 18, 2011, Arlington, VA

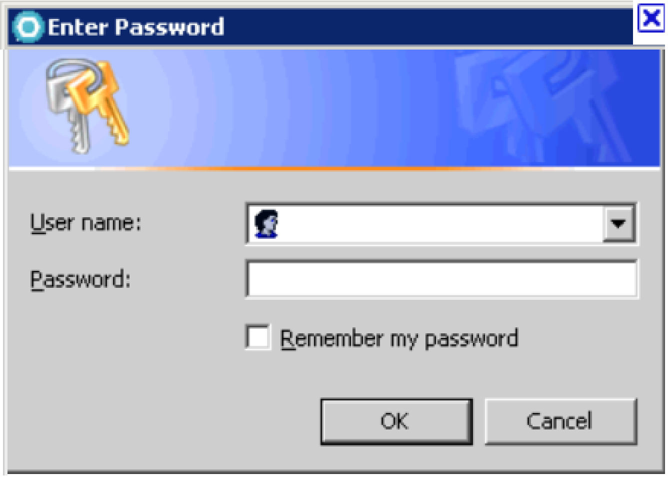
14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**23**	

How Computers Identify Us

Our present:



Enter Password

User name:

Password:

□ Remember my password

Our Future?

Source: http://us.123rf.com

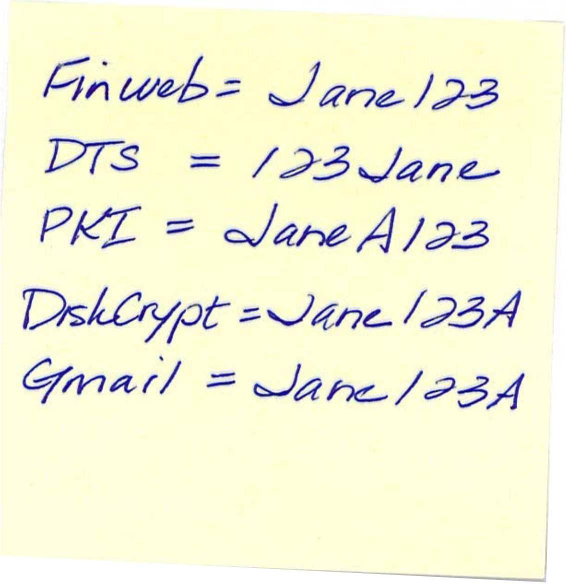
Active Authentication Program Goal

Computers watch their operators, and manage their level of access based on the accuracy with which they can determine the operator’s identity

Source: http:www.zuschlogin.com

Source: 2.bp.blogspot.com

Users are the weak link...



Finweb = Jane123
DTS = 123Jane
PKI = JaneA123
DiskCrypt = Jane123A
Gmail = Jane123A

How many passwords do we really use?

DoD IT Asset Type	DARPA Reference System
NIPRnet	Windows DMSS
Laptop Encryption	Guardian Edge
DARPA VPN	Nortel
PDA	Blackberry/iPhone
SIPRnet	Windows DSN
JWICS	Windows DJN
Source Selection	TFIMs, I2O BAA Tool
Contract Management	GSA Advantage, SPS
Contract Invoicing	Wide Area Workflow
Payroll	MyPay
● Benefits	Benefeds.com
HR	hr.dla.mil
● Training	DAU
● Collaboration	Defense Connect Online
Financial System, Local	Momentum
Financial System, Agency	DFAS
● Credit Union	PFCU, NCU, etc.

Non-DoD IT Asset Type	Hacked on	Credentials lost
American Honda Motor Co.	27-Dec-10	4.9m
● Bank of America	25-May-11	1.2m
Carnegie Mellon University	8-Oct-07	19k
Citigroup	27-Jul-10	30m
Clarkson University	10-Sep-08	245
● Countrywide Financial Corp.	2-Aug-08	17m
● Fidelity Investments	24-Sep-07	8.7m
Heartland Payment Systems	20-Jan-09	130m
IBM	15-May-07	2k
Johns Hopkins Hospital	22-Oct-10	152k
SAIC	7-May-08	630k
Sony	27-Apr-11	12m
Stanford University	6-Jun-08	82k
TD Ameritrade Holding Corp.	14-Sep-07	6.5m
Texas A&M University	9-Nov-08	13k
TJMax Stores	17-Jan-07	100m
U.S. Depart. of Veteran Affairs	14-May-07	103m
U.S. Marine Corp – PSU research	26-Jul-07	208k
● Visa, MasterCard, and American Express	27-Dec-10	4.9m

Source: www.privacyrights.org/data-breach

MSNBC News Report:
Cyber attack on Gannet Targets US Soldiers

Hackers broke into a Gannett Co database containing personal information about subscribers to publications read by U.S. government officials, military leaders and rank-and-file soldiers, the media company said on Tuesday.

Gannett told subscribers via email that it discovered the breach of its Gannett Government Media Corp on June 7. It said it had previously notified subscribers of the breach via a notice on its website.

The attackers accessed subscribers' names, passwords and email addresses, the company said. They also obtained data on the duty status, paygrade and branch of service of some readers who serve in the military.

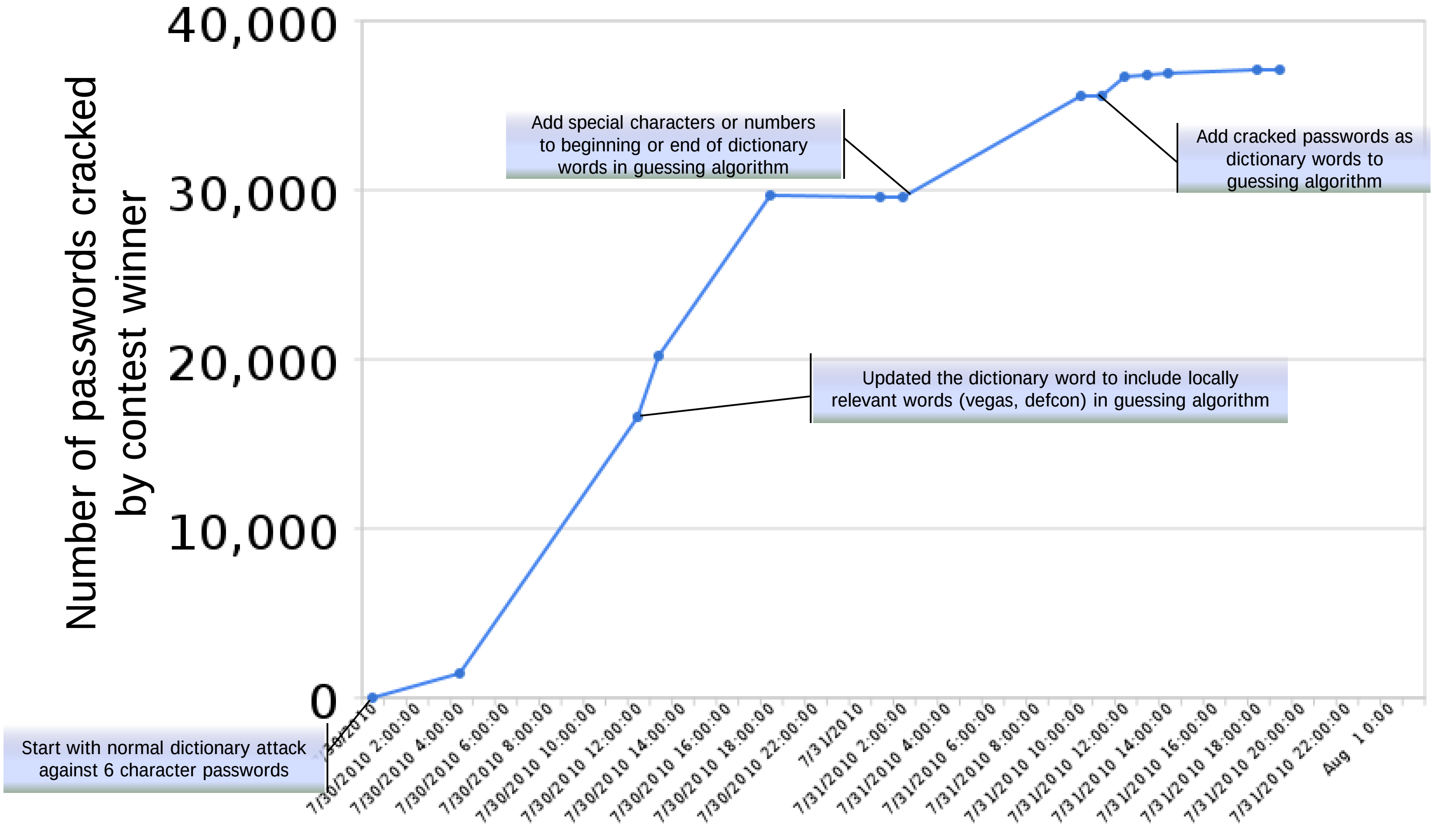
The information included subscribers to Defense News — one of the world's most widely read publications covering the defense industry — as well as publications aimed at soldiers serving in the U.S. Army, Navy, Air Force and Marine Corps.

By Jim Finkle
updated 6/28/2011 6:49:26 PM ET

Source: www.msnbc.msn.com

Patterns will always be hackable

Defcon 2010 Contest on Password Hacking of 53,000 passwords



Add special characters or numbers to beginning or end of dictionary words in guessing algorithm

Add cracked passwords as dictionary words to guessing algorithm

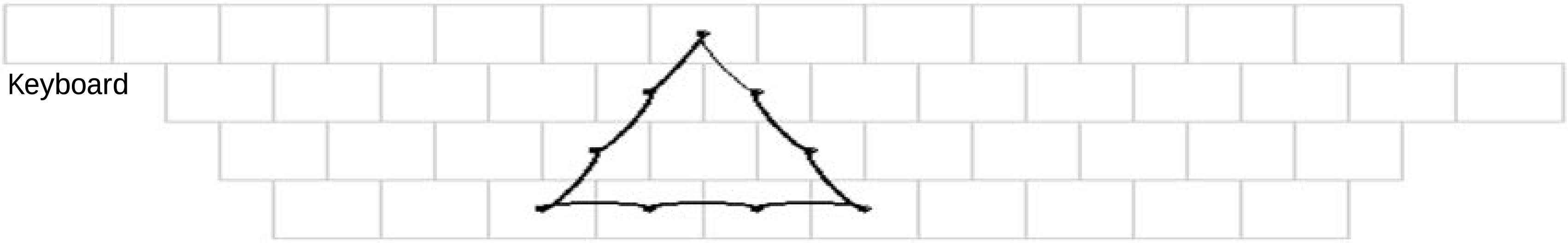
Updated the dictionary word to include locally relevant words (vegas, defcon) in guessing algorithm

Start with normal dictionary attack against 6 character passwords

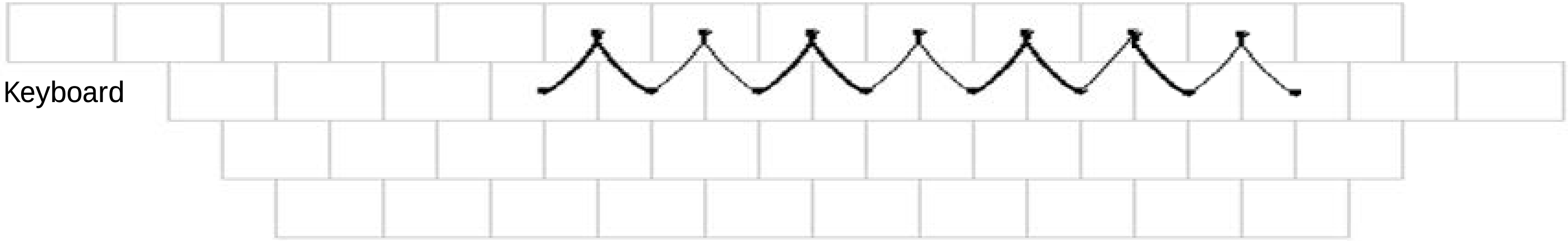
(2 hour increments over 48 hours)

Source: http://contest.korelogic.com/

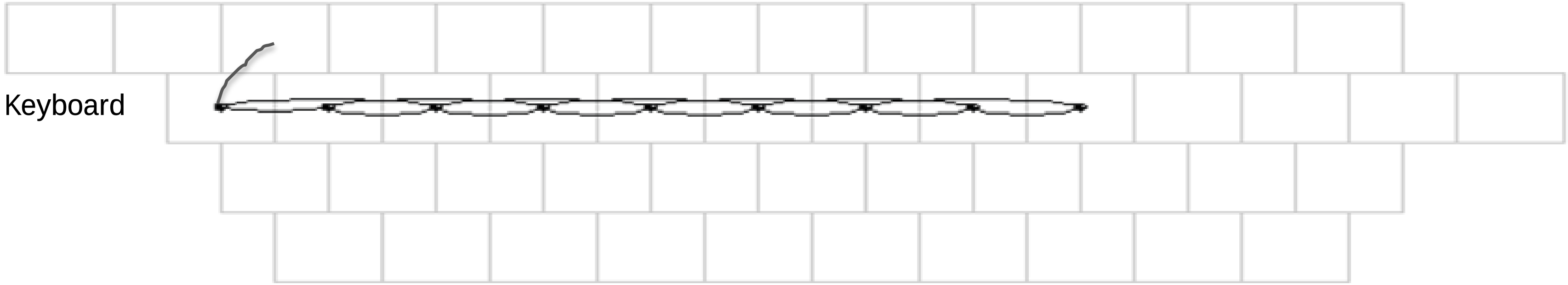
Why will passwords always be a problem?



6tFcVbNh^TfCvBn



R%t6Y&u8I(o0P-[



#QWqEwReTrYtUyI

Source: *Visualizing Keyboard Pattern Passwords*, US AF Academy 11 Oct, 2009

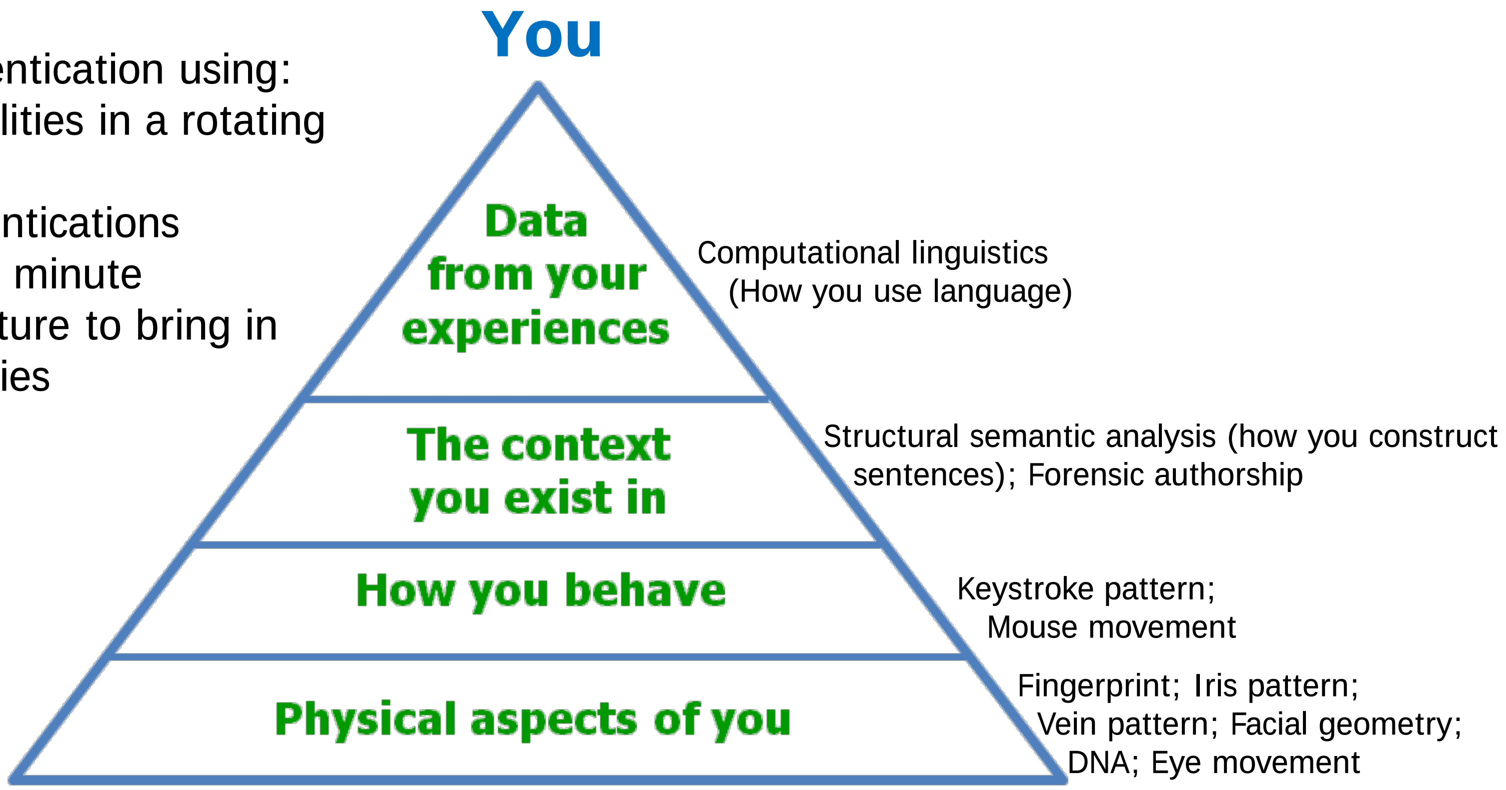
How do we move from proxies for you to the actual you?

Solution: **Active Authentication**

An open solution that provides **meaningful** and **continual** authentication to DoD's computer systems leveraging that which makes up **you**

Continuous authentication using:

- Multiple modalities in a rotating fashion
- Multiple authentications initiated each minute
- Open architecture to bring in future modalities



Computational linguistics (How you use language)

Structural semantic analysis (how you construct sentences); Forensic authorship

Keystroke pattern; Mouse movement

Fingerprint; Iris pattern; Vein pattern; Facial geometry; DNA; Eye movement

Transparent validation of the person at the computer
Without passwords
Without proxies
Without hassle

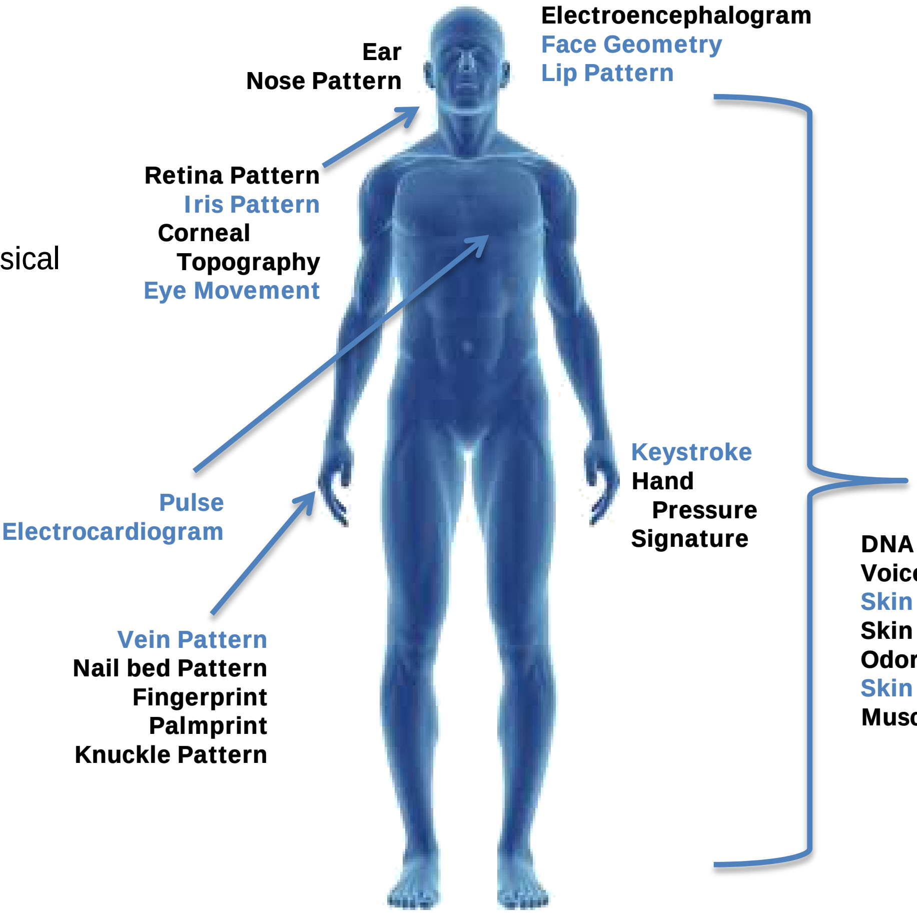
Existing Biometric Modalities

Current Solutions

Physiological Biometrics

Sensors tracking the physical attributes of you

- DNA
- Ear Geometry
- Facial Geometry
- Fingerprint
- Iris Pattern
- Knuckle Pattern
- Lip Pattern
- Nail bed Pattern
- Nose Pattern
- Oto-acoustic Emissions
- Palmprint
- Retina Pattern
- Skin Spectroscopy
- Vein pattern



Ear
Nose Pattern

Electroencephalogram
Face Geometry
Lip Pattern

Retina Pattern
Iris Pattern
Corneal Topography
Eye Movement

Pulse
Electrocardiogram

Keystroke
Hand Pressure
Signature

Vein Pattern
Nail bed Pattern
Fingerprint
Palmprint
Knuckle Pattern

DNA
Voice
Skin Thermography
Skin Spectroscopy
Odor
Skin Impedance
Muscle Movement

Behavioral Biometrics

Sensors tracking how you interact with the world

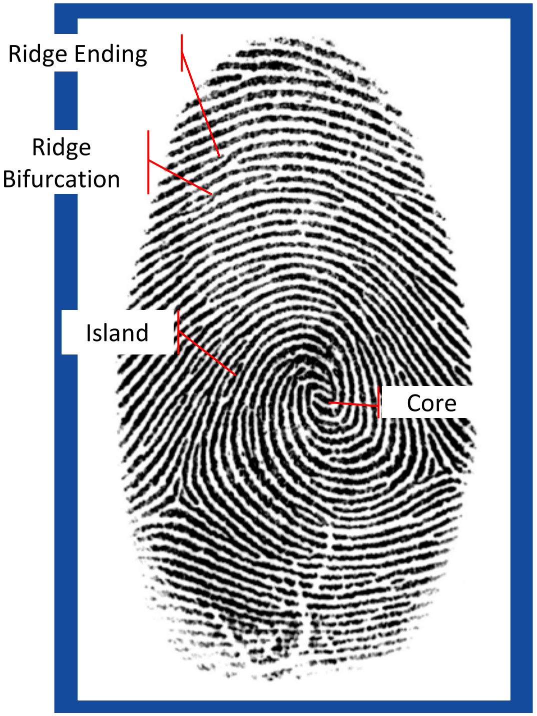
- Eye Movement
- Hand Pressure
- Keystroke pattern
- Signature
- Voice

Blue may be suitable for continuous monitoring
Black require interrupting the user

Biometric Identity Modalities

Physical aspects of you

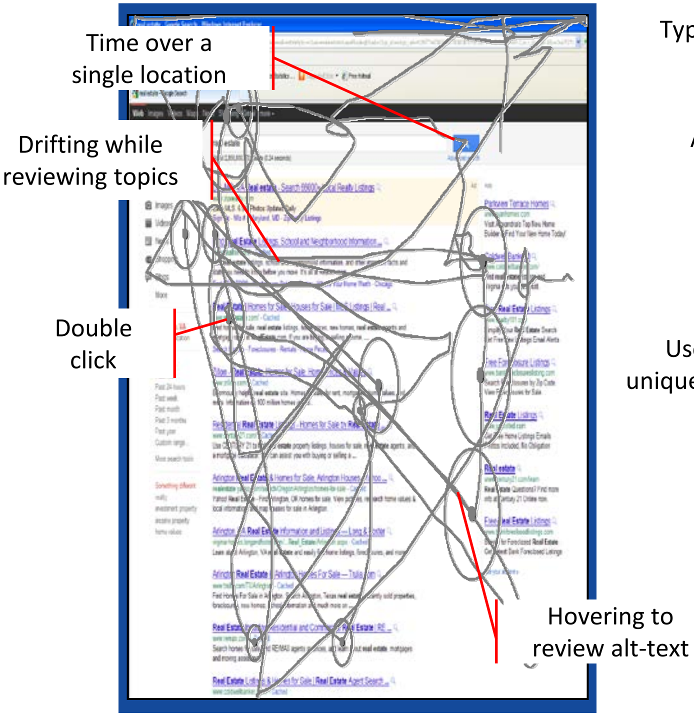
Fingerprint



Source: epdeatonville.org

How you behave

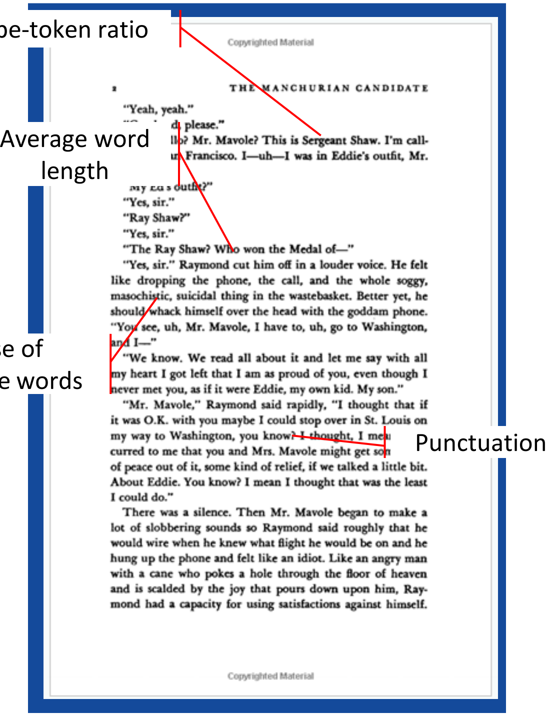
Mouse tracking[1]


Time over a single location
Drifting while reviewing topics
Double click
Hovering to review alt-text

Source: google search for "real estate" with mouse tracking provided by IOGraph

The context you exist in

Forensic authorship[2]


Type-token ratio
Average word length
Use of unique words
Punctuation

Copyrighted Material

2 THE MANCHURIAN CANDIDATE

"Yeah, yeah."

d, please."

llo? Mr. Mavole? This is Sergeant Shaw. I'm call-
n Francisco. I—uh—I was in Eddie's outfit, Mr.

My Ed's outfit?"

"Yes, sir."

"Ray Shaw?"

"Yes, sir."

"The Ray Shaw? Who won the Medal of—"

"Yes, sir." Raymond cut him off in a louder voice. He felt like dropping the phone, the call, and the whole soggy, masochistic, suicidal thing in the wastebasket. Better yet, he should whack himself over the head with the goddam phone. "You see, uh, Mr. Mavole, I have to, uh, go to Washington, and I—"

"We know. We read all about it and let me say with all my heart I got left that I am as proud of you, even though I never met you, as if it were Eddie, my own kid. My son."

"Mr. Mavole," Raymond said rapidly, "I thought that if it was O.K. with you maybe I could stop over in St. Louis on my way to Washington, you know? I thought, I mea
curred to me that you and Mrs. Mavole might get so
of peace out of it, some kind of relief, if we talked a little bit. About Eddie. You know? I mean I thought that was the least I could do."

There was a silence. Then Mr. Mavole began to make a lot of slobbering sounds so Raymond said roughly that he would wire when he knew what flight he would be on and he hung up the phone and felt like an idiot. Like an angry man with a cane who pokes a hole through the floor of heaven and is scalded by the joy that pours down upon him, Raymond had a capacity for using satisfactions against himself.

Copyrighted Material

Source: The Mancurian Candidate, Robert Graves, P2, Amazon Preview

[1] *What can a mouse cursor tell us more?: correlation of eye/mouse movements on web browsing*, Mon-Chu Chen, John R. Anderson, Myeong-Ho Sohn (all CMU), 31 March 2001

[2] *Quantifying evidence in forensic authorship analysis*, Dr Tim Grant, Aston University, UK 2007

Existing Technology

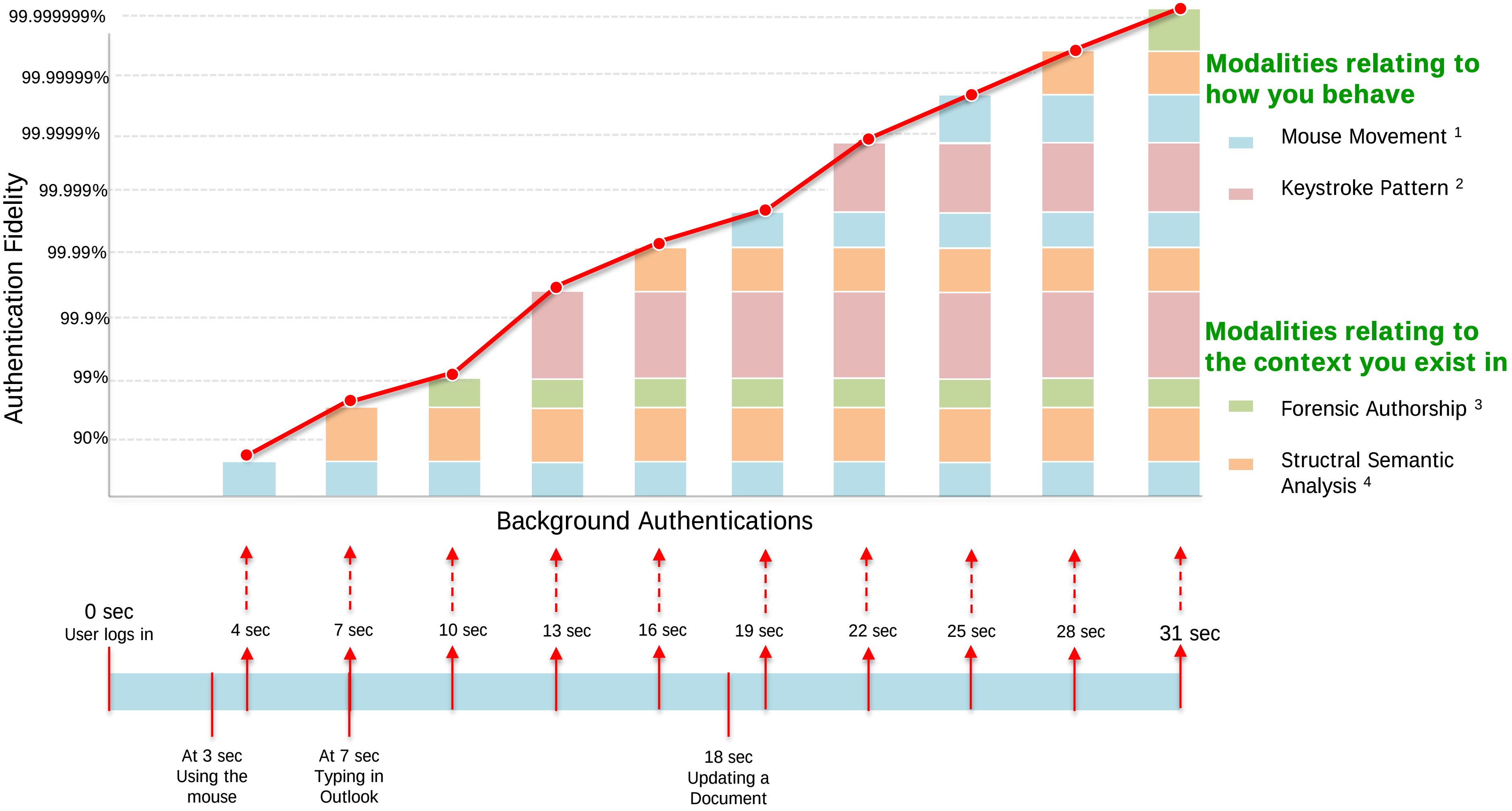
Repurposed Technology

New Technology

Layering Modalities – how it will work

- The Active Authentication Platform replaces the authentication framework within a desktop operating system with a protected framework
  - Ex: winlogon and GINA.DLL for Microsoft Windows
- The user will identify themselves and gain access to the system
- The Active Authentication Platform will then look for user activity, capturing biometric information as it is available
  - Ex:
    - Comparing the mouse when mouse activity occurs
    - Comparing the pattern of typing when the keyboard is used
    - Comparing word usage when documents are created
- As system trust in the identity of the user increases, access to more critical systems is made available
- When system trust is not high enough, the Active Authentication platform initiated a re-check process to validate the identity of the user and takes system admin direction as needed

Active Authentication Scenario



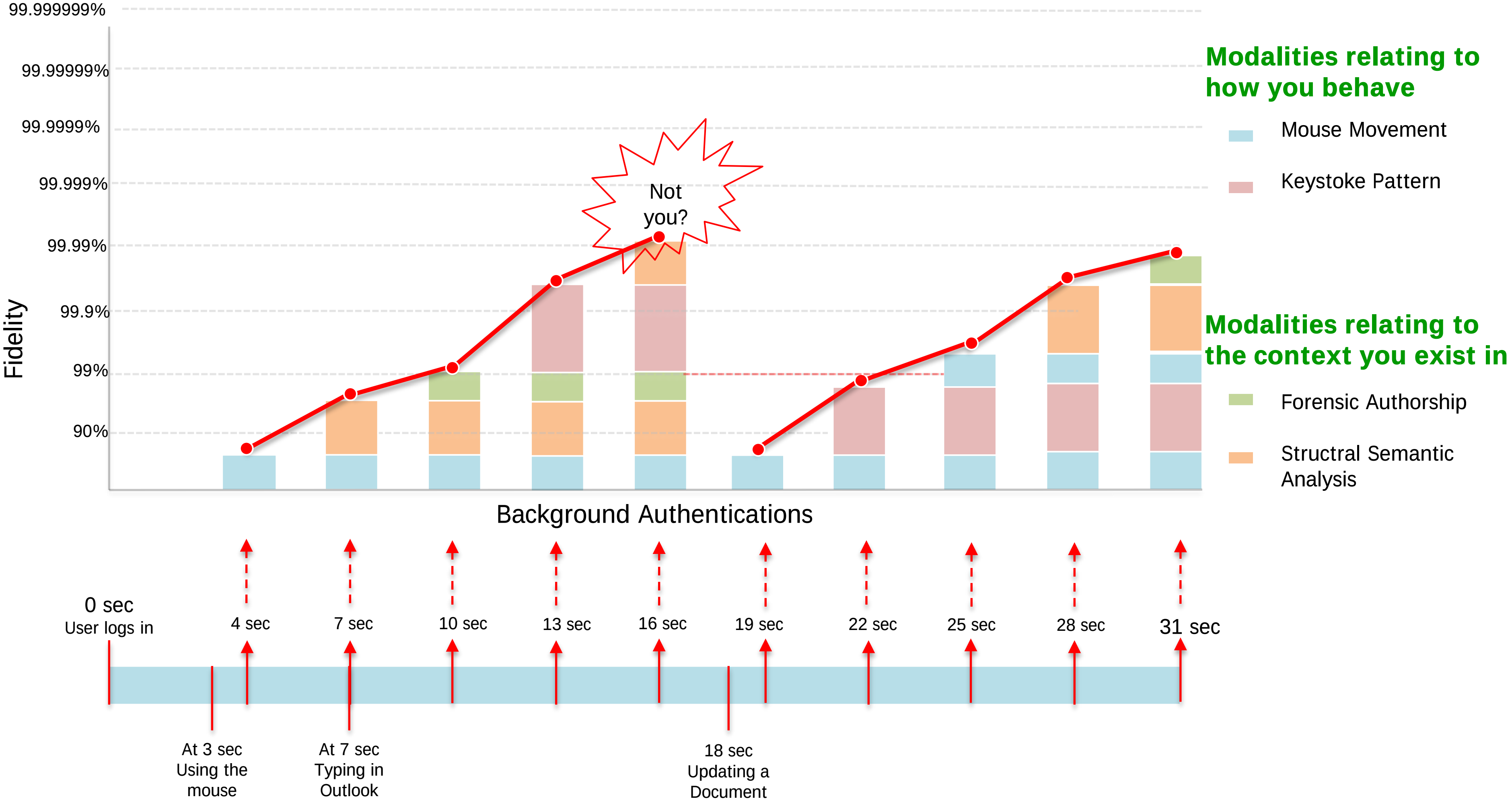
1 - Mouse Movement (Mon-Chu Chen, John R. Anderson, Myeong-Ho Sohn 2001) (73-80% True Positive Rate)

2 - Keystroke Pattern (Gunetti et. al., 2005) (94-95% True Positive Rate)

3 - Forensic Authorship (Dr Tim Grant, Aston University, UK 2007) (80-93% True Positive Rate)

4 - Structral Semantic Analysis (de Vel et. al., 2002) (86-91% True Positive Rate)

Active Authentication Scenario (“not you”)



Automatic system re-test to validate identity to a threshold set by system administrator (example uses 99% over 3 tests)

No user interruption until the system’s confidence level is breached (based on local thresholds set)
If it is breached the user is disconnected from all resources (local site chooses actions, logged off or disconnected)

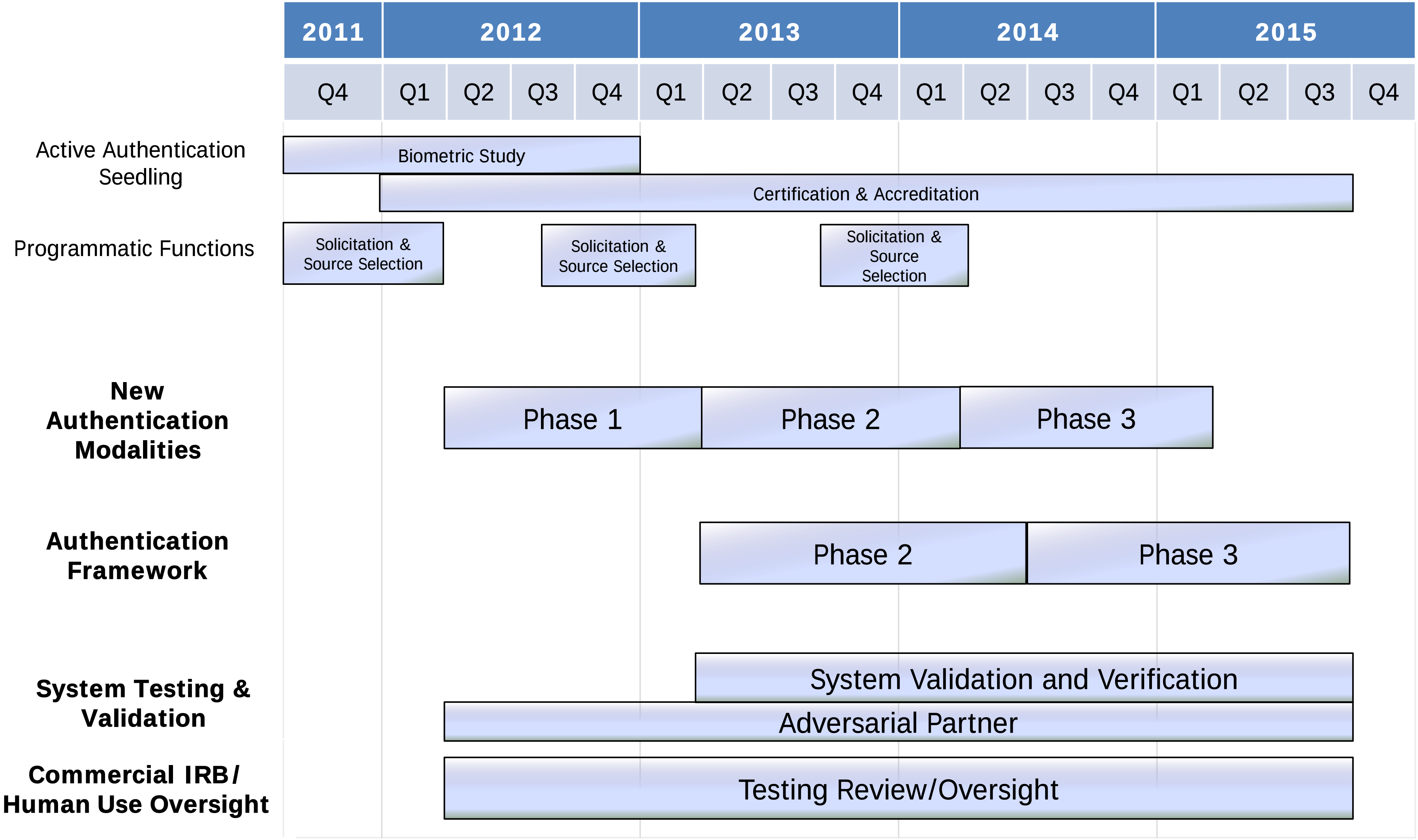
How do we measure success?

		Phase 1	Phase 2	Phase 3
Introduced new authentication modalities				
	Maximum False Rejections after five (5) scans	1/week	1/month	1/month
	True Positive Rate for each scan	80%	80%	85%
	Usability of modality within the population of DoD personnel	90%	90%	95%

***Note:** The Authentication Platform does not start until Year 2, and will be addressed in a later solicitation, below are planned metrics*

			Phase 1	Phase 2
Authentication Platform				
	Able to maintain a minimum True Positive Rate of 99.999% after:		45 sec	30 sec
	Number of integrated modalities		5	10
	Maximum response time to process a single authentication		12 sec	6 sec
	Number of authentications performed per minute (APM)		5	10

Active Authentication Program Plan



2011 | 2012 | 2013 | 2014 | 2015

Q4 | Q1 Q2 Q3 Q4 | Q1 Q2 Q3 Q4 | Q1 Q2 Q3 Q4 | Q1 Q2 Q3 Q4

Active Authentication Seedling

Biometric Study

Certification & Accreditation

Programmatic Functions

Solicitation & Source Selection

Solicitation & Source Selection

Solicitation & Source Selection

New Authentication Modalities

Phase 1

Phase 2

Phase 3

Authentication Framework

Phase 2

Phase 3

System Testing & Validation

System Validation and Verification

Adversarial Partner

Commercial IRB / Human Use Oversight

Testing Review/Oversight

Active Authentication Program focus areas

1. Emerging Authentication Modalities:
New methods for verifying a user's identity focusing on software biometrics in an office automation environment

2. Multifactor Authentication Integration:
Integration of the multiple modalities into a single platform for authentication developed in an open architecture to allow introduction of new solutions

Note: *The multifactor authentication integration focus area does not start until Year 2, and will be addressed in a later solicitation*

3. System Testing & Validation:
Both Independent Verification & Validation of the developed code and active Red Team analysis of the solution to ensure the solutions developed do not increase the current available attack surface

Phase 1 Activities

- The Solicitation is expected to come out in late November/Early December
- The Solicitation is currently expected to be open for 60 business days
- Multiple awards are expected for Technical Area #1
- Technical Area 2 will not be included in the Solicitation for Phase 1
- Multiple awards are not expected Technical Area #3

Technical Area #1
Emerging Authentication Modalities

- New biometric modality studies on software based biometrics that can capture aspects of the “cognitive fingerprint” that will be able to quantitatively their findings with human testing

- Expected to range from 3-6 months in length, but will all complete the end of Phase 1 (Q1 2013)

- Expected cost no more than $500K per study

- There will be a heavy focus on providing quantitative analysis of the new solutions through testing

- Quantitative analysis will be required for performers in Phase 2

Technical Area #3
System Testing & Validation

- Provide Red Teaming or “Adversarial Partner” Subject Matter Expertise for length of Active Authentication program

- Provide realistic picture of risk introduced with the new modality approaches

- The Level of Effort for this technical area is expected to be low for Phase 1, with a significant increase in Phase 2 and 3

- Both Independent Verification & Validation of the developed code and active Red Team analysis of the solution to ensure the solutions developed do not increase the current available attack surface

- IV&V functions do not start until Phase 2

Potential Future Applications

Tactical Uses

Military personnel in Mission Orientated Protective Posture (MOPP) level 4 have to endure passwords while wearing 2 pairs of gloves

Command and Control

Right before picking up the “Red Phone” is not the time you want to verify your system access!

Medical Safety

Because of time constraints, medical personnel currently have no active verification of proficiency training or authorization

Physical Security

How many times have you forgotten your badge?

Mobile and Commercial

Anywhere passwords are currently being used could be converted to active authentication via biometrics www.darpa.mil